REMARKS

Applicants thank the Examiner for the careful and thorough examination of the present application. Independent Claim 12 has been amended to correct a minor informality. The patentability of the claims is discussed below.

I. The Claimed Invention

The invention is directed to a cryptographic device. Independent Claim 1, for example, recites a cryptographic device, which includes a cryptographic module and a communications module coupled thereto. More particularly, the cryptographic module includes a user network interface, a host network processor coupled to the user network interface, and a cryptographic processor coupled to the host network processor. Additionally, the communications module includes a network communications interface coupled to the cryptographic processor. The host network processor generates cryptographic processor command packets for the cryptographic processor each having an address portion and a data portion, and it also encapsulates command packets for the communications module interface in the data portions of the cryptographic processor command packets. Moreover, the cryptographic processor passes the command packets to the communications module without performing cryptographic processing thereon. The user network interface includes a plurality of different connectors for coupling the cryptographic module to different network devices.

Independent Claim 21 is a method counterpart to independent Claim 1. Independent Claim 26 is a system counterpart to independent Claim 1 further reciting the host network processor formatting the data portions based upon the simple network management protocol.

Independent Claim 12 is directed to a cryptographic device as recited in independent Claim 1 further reciting the user network interface as a Local Area Network (LAN) interface, the command packets as Ethernet command packets, and the host network processor formatting the data portions based upon the simple network management protocol.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 12, 21, and 26 based on a combination of Dellmo et al., Stallings, and Dichter. Independent Claim 12 was rejected further in view of Stevens. Dellmo et al. is directed to a secure wireless LAN device including a housing, a wireless transceiver carried by the housing, and a cryptography circuit carried by the housing. A media access controller (MAC) is included and implements a predetermined wireless LAN MAC protocol. The cryptography circuit includes a cryptography processor, and a control gateway circuit connected to the MAC and the wireless transceiver. The secure wireless LAN device also includes a user network interface carried by the housing and connected to the MAC.

The Examiner correctly recognized that Dellmo et al. does not disclose the host network processor generating cryptographic processor command packets for the cryptographic processor each having an address portion and a data portion, and encapsulating command packets for the communications module interface in the data portions of the cryptographic processor command packets.

The Examiner then turned to Stallings for these noted critical deficiencies of the primary reference, Dellmo et al. Stallings is a general cryptography textbook, and the Examiner pointed particularly to the text on page 418, lines 8-13, which discloses encrypting IP packets for transmission through an Internet firewall:

> The source prepares an inner IP packet with a destination address of the target internal host. This packet is prefixed by an ESP header; then the packet and ESP trailer are encrypted and Authentication Data may be added. The resulting block is encapsulated with a new IP header (base header plus optional extensions such as routing and hop-by-hop options for Ipv6) whose destination address is the firewall; this forms the outer IP packet. (Emphasis added).

As previously noted, Dellmo et al. is directed to a secure wireless LAN device. A MAC is included and implements a predetermined wireless LAN MAC protocol. The cryptography circuit includes a cryptography processor, and a control gateway circuit connected to the MAC and the wireless transceiver. The secure wireless LAN device also includes a user network

interface connected to the MAC. In contrast, Stallings, although a general text, is directed to the case where an external host wishes to communicate with a host on an internal network protected by a firewall, and which ESP is implemented in the external host and firewalls (page 418, lines 3-5). A person having ordinary skill in the art would not turn to the ESP implemented network/firewall technology disclosed in Stallings to generate, process, and pass packets from the internal processors and modules on an ESP independent cryptographic device in Dellmo et al. Accordingly, the combination of Dellmo et al. and Stallings is improper.

Moreover, in Stallings, the resulting packet is encapsulated with a new IP header and has a destination address of the firewall (page 418, lines 11-13). Implementing Stallings into Dellmo et al. would destroy the functionality of Dellmo et al. since the packets are generated for passing between the cryptographic processor and the communications module internal to the device.

The Examiner also correctly recognized that even a combination of Dellmo et al. and Stallings fails to disclose the user network interface including a plurality of different connectors for coupling the cryptographic module to different network devices. The Examiner then turned to Dichter for this critical deficiency.

Dichter is directed to a computer network including a plurality of nodes. A programmable switching network allows the

nodes to be connected in a plurality of different ways, for example, to selectively allow a node to be connected either as a pass through node or a non-pass through node, and to connect nodes to one another via telephone lines.

Applicants respectfully submit Dichter fails to disclose the user network interface including a plurality of different connectors for coupling the cryptographic module to different network devices. The Examiner contends that a network hub, as disclosed in the background of Dichter, supplies the critical deficiency of Dellmo et al. As disclosed in the background of Dichter, a network hub includes "a plurality of cable connectors so that each computer on the network may be connected to the hub." (See Dichter, Col. 1, lines 32-34). The network hub, as disclosed in Dichter, fails to disclose or suggest that the connecters are different. In fact, Dichter discloses that the connectors of the hub are all the same, that is, they are all RJ-45 connectors. (See Dichter, Col. 1, lines 49-53). Accordingly, the Examiner's combination of references fails to disclose the claimed invention, as recited in the independent claims.

Additionally, Applicants respectfully submit that the Examiner's combination of Dellmo et al., Stallings, and Dichter is improper. Applicants point out that Dellmo et al., whose primary objective is to provide greater security in a wireless LAN environment, teaches a secure wireless LAN device including a housing, a wireless transceiver carried by the housing, and a

cryptography circuit carried by the housing. Conversely, Dichter discloses a configurable network that provides an efficient and specification compliant topology without requiring the rewiring of a building. A person having ordinary skill in the art would not turn to the programmably configurable computer network of Dichter to combine with the cryptographic device of Dellmo et al.

Still further, Dichter is directed to a wired computer network. As noted above, the wired configurable network of Dichter advantageously allows the use of existing wiring in a building, mainly existing telephone lines. In stark contrast, Dellmo et al. discloses a secure wireless network device. A person having ordinary skill in the art would not combine the wired network of Dichter with the secure wireless network device of Dellmo et al. as not only does Dichter teach away from Dellmo et al, but combining the wired network of Dichter with the secure wireless device of Dellmo et al. would destroy the operability of the Dellmo et al. secure wireless device.

Moreover, one having ordinary skill in the art would not turn to Stallings, a general text, which is directed to the case where an external host wishes to communicate with a host on an internal network protected by a firewall, to combine with the configurable computer network teachings of Dichter. Accordingly, the Examiner's combination of references is improper.

The Examiner also rejected independent Claim 12 over a four-way combination of Dellmo et al., Stallings, Dichter, and

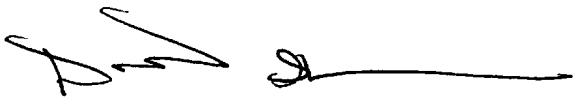
Stevens. Stevens is cited as disclosing an SNMP protocol. Stevens adds nothing to the critical deficiencies of Dellmo et al., Dichter, and Stallings.

Accordingly, it is submitted that the independent claims are patentable over the prior art. In view of the patentability of the independent claims, it is submitted that their dependent claims, which recite yet further distinguishing features, are also patentable over the cited references for at least the reasons set forth above. Accordingly, these dependent claims require no further discussion herein.

III. Conclusions

In view of the arguments presented above, it is submitted that all of the claims are patentable. Accordingly, a Notice of Allowance is therefore respectfully requested in due course. If the Examiner determines any remaining informalities exist, he is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



DAVID S. CARUS
Reg. No. 59,291
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Attorney for Applicants